



Fernando de la Cuadra
International Technical Editor
Panda Software (<http://www.pandasoftware.com>)
E-mail: Fdelacuadra@pandasoftware.com



Defenses against new viruses

Fourteen years ago, Panda Software started out in the world of antivirus software. Its first product was a simple antivirus program which was able to detect three viruses! Hardly a spectacular number, and some way short of the 70,000 viruses currently in existence, but in 1990 it was more than enough to meet users' basic requirements. We should remember that at the time personal computers were not nearly as widespread as they are now – in fact, they were viewed as something of a luxury – and few companies were as computerized as today's organizations.

As the years went by, the technology used to detect viruses improved markedly. Virus creators became increasingly skilled at ensuring that their code went undetected by antivirus programs, while antivirus software developers created new methods of detection and disinfection.

As the Internet became more popular, administrators saw how viruses were beginning to spread through channels which were inaccessible to traditional antivirus software. Email, for example, provided an inexhaustible supply of virus scares for networks with antiquated antivirus protection.

And viruses grew from being a local problem to becoming a global plague. Thanks to the Internet, the propagation of individual viruses was no longer restricted to specific areas, and borders became little more than an irrelevance.

Another very important factor was the speed with which the new viruses spread. While in the beginning a virus might take months to spread, thanks to the Internet this was reduced to a few days. Updating software against new viruses became more vital than ever, until daily updates were necessary.

Recently, we have seen a new challenge in the world of antivirus technology. Threats don't need months or even days to spread: a few minutes is enough! Codes such as SQLSlammer, Blaster or Sasser can spread so rapidly that users don't even have time to react. Virus creators know that there is a period during which computers are defenceless, and they seek to ensure that the viruses attack at precisely this moment.

A classic antivirus system detects viruses using the features of each individual code. Just like a genetic code, each virus code contains some bytes which are unique and unrepeatable, and the software uses these to search for the virus. However, as noted above, time is required to distribute the antivirus update which allows the program to detect and eliminate the virus.

The solution to new viruses cannot be based on detecting them only once they have appeared, because this doesn't give enough time to stop them. Instead, it must be based on what viruses may do. If we look at the behavior of the viruses mentioned above, all of them exploited some kind of vulnerability in the operating system, and this fact also points the way towards a solution. I'm not thinking of the traditional method of applying software "patches"; while this can be 100% effective in preventing infections, it is impossible to implement this solution quickly enough. Instead, what I have in mind is monitoring the exploitation of vulnerabilities.

Sasser, to cite the most recent example, exploited a vulnerability in order to cause a buffer overflow. If a system is installed on the computer which monitors any tasks which are being executed and their activity when interacting with the operating system, it is possible to prevent inappropriate use of the program data pile (the buffer) which may harm the system. The idea is not a new one. When boot viruses were widespread, many manufacturers of motherboards developed "antivirus" systems simply by recording programs which prevented writing to the boot sectors of disks. This is a basic form of protection which attempts to prevent the action of the virus instead of detecting and removing it.

Future protection against malicious codes based on monitoring processes is the key to being able to protect both individual computers and entire networks against the new fast-moving threats. Working in tandem with traditional antivirus software, and being supported by the antivirus companies' system of monitoring and development to provide almost instant responses to any suspected viruses which are received is, without question, the way to provide the protection companies need.

However, not all today's antivirus software developers are able to offer these new technologies. Instead, they will only be offered by those companies with Research & Development & innovation departments (R&D&i) which are working on these technologies and which have successfully detected the problem in advance.

Fernando de la Cuadra
International Technical Editor
Panda Software (<http://www.pandasoftware.com>)
E-mail: Fdelacuadra@pandasoftware.com